State of Iowa Enterprise Data Classification Standard

December 14, 2006

Purpose

This standard establishes a requirement for participating agencies to classify all data they collect, store, process or share with others. Common classifications include confidential, sensitive and public. At a minimum, agencies should separate data into confidential and public classifications, but other classifications may be used where applicable. Once data are classified, it is possible to make decisions about how those data will be protected, stored, transmitted or shared.

Overview

The State of Iowa collects and manages vast quantities of information. Some of the information is confidential, meaning state or federal law prohibits sharing the information with unauthorized individuals or groups. Some information may not be explicitly protected by law, but should still be protected because unauthorized access could result in negative consequences for the state, its partners or its citizens. Information is assumed to be public unless the agency has included it in a non-public classification.

Scope

This standard sets a timeline within which all state agencies must review the data they manage and classify all data into confidential and public classifications, plus any others they deem appropriate. The standard also requires agencies establish appropriate protection measures for data in each classification type.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Data Classification Standard are defined below:

- **Data Classification System:** The classification of all data stored, processed or transmitted into categories based on the extent to which they must be protected.

Enterprise Data Classification Standard

1. **Data Classification.** All data and the information derived from data must be classified by the level of protection required. At a minimum data should be classified as either public or confidential. If additional classifications are needed to meet agency requirements, they should be defined clearly within the classification system. For example, some organizations have a category of "sensitive."

    - Confidential: Protected by state or federal law.
    - Sensitive: Not explicitly protected by law, but exposure could result in negative impact to government services, state government partners or citizens.
    - Public: Data not included in a protected classification.

2. **Agency Standard for Protection of Data Classes:** Each agency shall set standards for protection for each data classification. Protections should consider different states of data; i.e. at rest, in transit and in use. All forms of the data must be considered; e.g. in local and networked databases, documents, spreadsheets, messaging, and on paper. Backup media must also be addressed.

3. **Assessment.** The ISO may assess agency compliance with this standard. Agencies will provide access to classification standard and documentation on how specific data are classified. If violations of this standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

4. **Notification:** On or before the effective date of this standard, agencies will provide the Chief Information Security Officer with a description of how they are classifying data and a description of the agency standard for protecting data in each classification type,

Effective Date
Agencies must be fully compliant with this standard no later than August 1, 2007. However, they are encouraged to implement this standard as soon as possible to help protect critical data assets.

Enforcement
This standard will be enforced per IAC 11--25.11(8A).